Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 7
- Proposed Solution -

Friday, May 31, 2019

Solution of Problem 1

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

a) Let $n = p$ be prime. It follows for the multiplicative group that:

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p-1\} \Rightarrow \varphi(p) = p - 1\,.$$

b) The power p^k has only one prime factor. So p^k has a common divisors that are not equal to one: These are only the multiples of p. For $1 \le a \le p^k$:

$$1 \cdot p\,, \quad 2 \cdot p\,, \quad \dots\,, \quad p^{k-1} \cdot p = p^k\,.$$

And it follows that

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)\,.$$

c) Let $n = p\,q$ for two primes $p \neq q$. It holds for $1 \le a < p\,q$

1) $p \mid a \vee q \mid a \Rightarrow \gcd(a, p\,q) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd(a, p\,q) = 1$.

It follows $\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \le a \le p\,q - 1\}}_{p\,q-1 \text{ elements}} \setminus \left\{ \underbrace{\{1 \le a \le p\,q - 1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \le a \le p\,q - 1 \mid q \mid a\}}_{p-1 \text{ elements}} \right\}$.

Hence: $\varphi(p\,q) = (p\,q - 1) - (q-1) - (p-1) = p\,q - p - q + 1 = (p-1)(q-1) = \varphi(p)\,\varphi(q)$.

d) Apply the Euler phi-function on n with the following steps:

1. Factorize all prime factors of the given n
2. Apply the rules in a) to c), correspondingly.

$\varphi(4913) = \varphi(17^3) \overset{\text{(b)}}{=} 17^2(17-1) = 4624$, and
$\varphi(899) = \varphi(30^2 - 1^2) = \varphi((30-1)(30+1)) = \varphi(29 \cdot 31) \overset{\text{(c)}}{=} 28 \cdot 30 = 840$.

Solution of Problem 2

Consider the set $\mathbb{Z}_{mn} = \{1, \ldots, mn\}$. If $x \in \mathbb{Z}^*_{mn}$ then $\gcd(x, m) = \gcd(x, n) = 1$. The members of $\mathbb{Z}_{mn}$ can be written as $am + b$ for $a \in \{0, 1, \ldots, n-1\}$ and $b \in \{1, \ldots, m\}$ namely:

$$\begin{array}{cccc}
0 \times m + 1 & 0 \times m + 1 & \ldots & 0 \times m + m \\
1 \times m + 1 & 1 \times m + 1 & \ldots & 1 \times m + m \\
\vdots & \vdots & \ddots & \vdots \\
(n-1) \times m + 1 & (n-1) \times m + 1 & \ldots & (n-1) \times m + m
\end{array}$$

For each $b_i \in \mathbb{Z}^*_m$, $am + b_i$ is also relatively prime with respect to m for $a \in \{0, 1, \ldots, n-1\}$. Hence in each row of the table above there are $\varphi(m)$ numbers relatively prime with respect to m. These numbers correspond to the columns $b_i \in \mathbb{Z}^*_m$ of the table above.

Now consider the column $am + b_i$ for $a \in \{0, 1, \ldots, n-1\}$. Since $\gcd(m, n) = 1$, all $am + b_i$'s are n different numbers modulo n among which only $\varphi(n)$ are relatively prime with respect to n. Therefore you have $\varphi(m)$ columns and in each column $\varphi(n)$ elements that are both relatively prime with respect to m and n. Therefore there are $\varphi(m)\varphi(n)$ numbers relatively prime to mn. Hence,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Solution of Problem 3

a) Define event A : 'n composite' $\Leftrightarrow \bar{A}$: 'n prime'.
Define event B : m-fold MRPT provides 'n prime' in all m cases.
From hint: $P(\bar{A}) = \frac{2}{\ln(N)} \Rightarrow P(A) = 1 - \frac{2}{\ln(N)}$ (cf. Thm. 6.7)

Probability for the case that the MRPT fails for m times:

$$P(B \mid A) \leq \left(\frac{1}{4}\right)^m$$

Probability of the MRPT verifying an actual prime is:

$$P(B \mid \bar{A}) = 1$$

Probability of the MRPT wrongly verifying a composite n as prime after m tests is:

$$\begin{aligned}
p &= P(A \mid B) \\
&= \frac{P(B \mid A) \cdot P(A)}{P(B)} \\
&= \frac{P(B \mid A) \cdot P(A)}{P(B \mid A) \cdot P(A) + P(B \mid \bar{A}) \cdot P(\bar{A})} \\
&\leq \frac{(\frac{1}{4})^m (1 - \frac{2}{\ln(N)})}{(\frac{1}{4})^m (1 - \frac{2}{\ln(N)}) + 1 \cdot \frac{2}{\ln(N)}} \\
&= \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}
\end{aligned}$$

b) Note that the above function $f(x) = \frac{x}{x+a}$ is monotonically increasing for $x \in \mathbb{R}$, $a > 0$, as its derivative is $f'(x) = \frac{a}{(x+a)^2} > 0$. Let $x = \ln(N) - 2$, and $N = 2^{512}$.
Resolve the inequality w.r.t. m:

$$\begin{aligned}
\frac{x}{x + 2^{2m+1}} &< \tfrac{1}{1000} \\
\Leftrightarrow 2^{2m+1} &> 999x \\
\Leftrightarrow m &> \tfrac{1}{2}(\log_2(999x) - 1) \\
\Leftrightarrow m &> \tfrac{1}{2}(\log_2(999(512\ln(2) - 2)) - 1) \\
\Leftrightarrow m &> 8.714.
\end{aligned}$$

$m = 9$ repetitions are needed to ensure that the error probability stays below $p = \frac{1}{1000}$ for $N = 2^{512}$.